

OS Registry

MEMORANDUM FOR: Executive Assistant/DDA

FROM:

Acting Executive Officer/OS

SUBJECT: Status: Implementation at CIA of NTISSP #2,
National Policy on Protection of Sensitive,
but Unclassified Information in Federal
Government Telecommunications and Automated
Information Systems

1. Representatives of the Office of Security, Office of Information Technology, Office of Information Services, and the Office of Communication have met to develop initial approaches as to how the policy is applicable at CIA and what, if any, might be the resource implications. The following pertinent points resulted:

° a. There is much less of a problem at CIA than at DoD and elsewhere because CIA contributes much less to technical data bases. Nonetheless, CIA does contribute to NTIS and probably economic and other data bases. OIT and OS have collected a listing of unclassified data bases which would provide a starting place for identifying those which contain sensitive but unclassified information. Once such a determination is made, the sensitive information should be removed from the system. If removal is not possible or practical, the system should be flagged in some way so that controls can be applied when and if the information is moved to an uncontrolled environment. Managers of each data base would have to assume responsibility for implementing any controls.

° b. A Headquarters Notice could serve to notify managers of the procedures, some of which would be incorporated into the permanent regulatory system. The Office of Security is beginning work on a Headquarters Regulation which will prescribe basic computer security standards; appropriate requirements for sensitive but unclassified information could be included. In a similar vein, the Office of Communications has prepared a draft Notice addressing

~~CONFIDENTIAL~~

CONFIDENTIAL

the protection of sensitive but unclassified information being transmitted via unclassified telecommunications links to and from CIA facilities and contractors.

° c. Much unclassified data is disseminated to or accessed by contractors through modems, the electronic interfaces through which the data is transmitted. Although contractors do not have access to CIA mainframe computer systems, the uncontrolled use of modems is inherently dangerous from a security standpoint. Work is presently being done, principally by OIT and OC, toward creating a Modem Pool which would provide for better security and would permit an audit trail to be created of Agency accesses to outside data bases. The modem pool would also provide us with a better way to control unclassified links to the outside and would prevent the use of unauthorized modems.

° d. Other unclassified information is disseminated from CIA on magnetic media, on paper and through oral presentations. Existing discipline, audit and distribution controls should suffice if we apply the above added procedures and enhance awareness.

° e. Guidance similar to the above would be prepared for CIA contractors.

25X1

2. The approach listed above consists of surveying the data bases, enhancing awareness of the problem and making modest procedural and regulatory changes. This should not prove costly if phased in slowly, appears to have security benefit and is likely to satisfy the basic requirements of NTISSP #2. The group's initial view is that other approaches, such as applying physical and technical security measures or requiring extensive or continuing surveys and audits, could not be accomplished with existing people and funds and would not be cost effective when measured against the sensitivity of the information to be protected. The key is manager awareness.

25X1

25X1 3. Other existing and planned programs for the protection of classified information are also, in part, responsive to the direction of NTISSP #2. Examples are Operations Security (OPSEC) and Computer Security (COMPUSEC) programs.

CONFIDENTIAL

4. The portion of Section IV - Responsibilities, which pertains to the DCI's responsibility to identify and protect sensitive but unclassified information bearing on intelligence sources and methods, was added, I believe, without CIA coordination. I presume it was well intentioned but, like much of NTISSP #2, is open to interpretation. Presuming that this portion includes protection of information bearing on Sensitive Compartmented Information, I have requested that the issue be broached at the DCI Forum as the responsible entity for preparation of a DCID or other appropriate action.

5. As we agreed during our telephone conversation we will proceed to coordinate appropriate regulatory issuances in concert with the Offices of Communications and Information Technology with at least a general policy issuance (Headquarters Notice) completed by 20 March 1987.

!OS/EO/PPS (25 Feb 87) !

!Distribution:!

Orig - Addressee

! 1 - OS/Registry!
! 1 - PPS Chrono!

OIT/Mgt. Div.!
- OC/ESG/CSS!
- IRMD/OIS!
- ISSD/OS!

CONFIDENTIAL